REMARKS

Claims 21-43 are pending. Claims 21, 28, and 35 are independent. Claims 21-22, 29, and 36 are amended for clarity and to correct minor typographical errors. The claim amendments do not change the scope of the respective claims. No new matter is added. Reconsideration of the action mailed January 12, 2006, is requested in light of the foregoing amendments and the following remarks.

The Examiner has stated that claims 42 and 43 are allowable. Applicant appreciates the Examiner's identification of allowable subject matter in claims 42 and 43.

The Examiner rejected claims 21-41 under 35 U.S.C. § 102(a) as being anticipated by NIST Special Publication 800-19-Mobile Agent Security ("Jansen"). Applicant respectfully traverses the rejections.

Section 102 Rejections

Claims 21 stands rejected over Jansen. Claim 21 is directed to a system that includes a server in communication with a first host and a second host. The first and second hosts execute a mobile application that jumps from the first host to the second host during execution, where during the jump from the first host to the second host the mobile application passes through the server.

Prior to the jump from the first host to the second host, the server stores a first instance of the mobile application. An instance of the mobile application includes executable code for the mobile application. During the jump to the second host, the server receives a second instance of the mobile application from the first host. The server detects unwanted changes in the contents of the mobile application including comparing the first and second instances of the mobile application.

The Examiner states that Jansen discloses a server storing a first instance of the mobile application prior to a jump to a second host at page 2, second paragraph and FIG. 1. Applicant respectfully disagrees. Page 2, second paragraph reads, in pertinent part, is as follows:

> A number of models exist for describing agent systems [2, 6, 7]; however, for discussing security issues it is sufficient to use a very simple one, consisting of

> only two main components: the agent and the agent platform. Here, an agent is comprised of the code and state information needed to carry out some computation. Mobility allows an agent to move, or hop, among agent platforms. The agent platforms provide the computational environment in which an agent operates. The platform from which the agent originates is referred to as the home platform, and normally is the most trusted environment for an agent. One or more hosts may comprise an agent platform, and an agent platform map support several computational environments, or meeting places, where agents can interact.

The portion of Jansen relied on by the Examiner describes only a simple model for describing an agent system where an agent represents a mobile application and agent platforms represent hosts. Nowhere in the portion relied on by the Examiner, however, is there any mention of a server or the claimed functions performed by Applicant's server. Similarly, FIG. 1 depicts the model discussed in the above cited paragraph. FIG. 1 simply does not include any server. Indeed, the arrow representing the path of travel of the mobile application in FIG. 1, *i.e.*, from one platform directly to another platform, indicates that the simple model described is peer to peer and not client to server. Thus, Applicant respectfully asserts that the portion indicated by the Examiner not only fails to mention, teach or suggest a server, but also teaches away from a client server model as set forth in claim 21 by showing a peer to peer model where a mobile agent jumps from host to host. There is no teaching in Jansen of a client server model that includes Applicant's claimed server performing the storing and detecting steps. Indeed, the Examiner appears to agree with Applicant's understanding of Jansen on page 2 of the Action when citing the above portion of Jansen where the Examiner explains the rejection by stating, "pg. 2, 2nd paragraph teaches Mobile agents (MA) hopping from ***peer to peer***" (emphasis added).

Additionally, Applicant respectfully asserts that Jansen (and particularly the portions of Jansen relied on by the Examiner) fail to teach or suggest a server storing, prior to the jump from the first host to the second host, a first instance of the mobile application where an instance includes executable code for the mobile application. There is no teaching or suggestion in Jansen to storing anything associated with the agent application. Furthermore, there is no teaching or suggestion to storing executable code for the mobile application in a server. As described above, Jansen as understood by the Applicant shows a peer to peer system. No storage

or involvement of a server appears required or desirable in Jansen. For this reason alone, claim 21 is allowable over Jansen.

The Examiner in his response to Applicant's previous arguments has indicated that Applicant's storage of executable code is taught in Jansen's itinerary. Applicant respectfully disagrees. First, Applicant respectfully asserts that an itinerary is not the same as Applicant's claimed executable code. Jansen's itinerary includes only a list of allowed hosts that the agent application can be executed on.

The itinerary disclosed at page 19 suggests that the originator of an agent (*i.e.*, the creator of a mobile application) can restrict which agent platforms (*i.e.*, hosts) the agent can jump to by defining a list of trusted agent platforms. *See* page 19, lines 3-7. Thus, the itinerary simply identifies a list of trusted agent platforms from which the agent can jump. There is no teaching or suggestion that the itinerary includes any executable code. Second, there is no teaching or suggestion of storing the itinerary on a server prior to the first jump. In fact, the sentence prior to the sentence relied upon by the Examiner in maintaining this rejection refers to an agent system with decentralized mobility, in other words, an agent system without a centralized server. For all of these reasons, Applicant respectfully asserts that Jansen fails to teach or suggest Applicant's claimed storing and detecting steps.

The Examiner also states that Jansen discloses a server detecting unwanted changes in contents of the mobile application including comparing the first and second instances at section 2.1.2, section 3.2, page 9, and section 4.2.2. Applicant respectfully disagrees.

Section 2.1.2 of Jansen discloses a type of threat referred to as a denial of service attack to an agent platform. Specifically, Section 2.1.2 states "Mobile agents can launch denial of service attacks by consuming an excessive amount of the agent platform's computing recourses.... Depending on the level of access, the agent may be able to completely shutdown or terminate the agent platform" (Section 2.1.2).

Thus, Section 2.1.2 discloses a specific type of threat to an agent system. However, the discussion of a type of security threat does not teach or suggest Applicant's claimed detection of unwanted changes in a mobile application. Denial of service is a particular type of security

attack. Such an attack could be launched if the code portion of a jumping application was modified. That said, nothing in Jansen teaches or suggests detecting such a code change. Jansen merely makes reference to a type of attack. Jansen is silent as to how to detect such an attack. There is absolutely no suggestion that mere possibility of a denial of service attack includes Applicant's claimed comparing of a first and a second instance of a mobile application on a server.

The Examiner also states that section 3.2 of Jansen discloses the determining step of claim 21. Section 3.2 of Jansen discloses integrity, which is one of four security requirements for networked computer systems. *See* page 8, section 3 "security requirements". Section 3.2 discloses that an agent platform must protect agents from unauthorized modification of agent code, state, and data. Furthermore, the agent platform must ensure that only authorized agents or processes are used to modify shared data. *See* page 9, last paragraph. The secure operation of the mobile agent depends on the integrity of the local and remote agent platforms. *See* page 10, first paragraph. Therefore, system access controls must be in place for agent platforms. *See* page 10, second paragraph. Additionally, section 3.2 also discloses attacks directed against messages sent intra or inter-platform with the goal of compromising system integrity. *See* page 10, third paragraph.

However, the cited section of Jansen is silent on any particular actions taken by a server to detect changes in a mobile application. The cited section of Jansen fails to teach or suggest the use of a server to detect unwanted changes in contents of a mobile application. Furthermore, the cited section fails to teach or suggest any comparison between first and second instances of a mobile application to detect changes in the contents of the mobile application.

The Examiner also states that section page 9 of Jansen discloses the determining step of claim 21. Page 9 includes most of section 3.1, which discloses confidentiality, which is a second of the four disclosed security requirements. Section 3.1 discloses the role of confidentiality in a network system. Specifically, section 3.1 discloses that private data stored on an agent platform or carried by an agent must remain confidential. *See* page 8, last paragraph. Eavesdroppers can gather information about an agent's activities not only from the content of messages being

exchanged, but also from message flow from one agent to another. *See* page 8 last paragraph. Mobile agents, thus, may want to keep their location confidential. *See* page 9, first full paragraph. Furthermore, audit log content must be kept confidential. *See* page 9, first full paragraph.

Again, while the cited section discloses the need for network security in keeping information confidential, there is no teaching or suggestion of providing confidentiality by detecting unwanted changes in contents of a mobile application on a server. Furthermore, there is no teaching or suggestion in the cited section that a first instance and a second instance of the mobile application are compared in order to detect unwanted changes, as required by claim 21.

Finally, Examiner states that section 4.2.2 of Jansen also discloses the determining step of claim 21. Section 4.2.2 of Jansen discloses mutual itinerary recording. Mutual itinerary recording is a scheme in which an agent records and tracks a peer agent's itinerary and vice versa. Specifically, when moving between platforms, the agent sends information regarding the last platform, current platform, and next platform to the peer agent. *See* page 21, second paragraph. The peer agent takes appropriate action when inconsistencies are detect. *See* page 21, second paragraph.

Section 4.2.2 of Jansen does not teach or suggest a server that detects unwanted changes in contents of a mobile application. Furthermore, section 4.2.2 of Jansen does not teach or suggest comparing a first and second instance of the mobile application to detect unwanted changes. The itinerary is not an instance of the mobile application. Furthermore, an itinerary is simply data and does not include executable code of for the mobile application, as required by claim 21.

Additionally, in the Examiner's responses to the Applicant's previous argument, the Examiner does not address any of the Applicant's arguments directed to section 2.1.2, section 3.2, page 9, or section 4.2.2 of Jansen, which were relied upon by the Examiner. Instead, the Examiner, despite maintaining the rejection based on those portions of Jansen, responds with a citation of page 19. The Examiner states that page 19 of Jansen discloses a central host allowing tampering to be detected. The Applicant respectfully disagrees. The only statement on page 19

regarding a central host is a brief mention of alternative systems that use a client-server structure. Specifically, the pertinent portion of page 19 reads as follows:

> For example, the Jumping Beans [43] agent system address some security issues by implementing a client-server architecture, whereby an agent always returns to a secure central host first before moving onto any other platform.

The next sentence following the quoted portion above changes the discussion to security for decentralized system (*i.e.*, peer to peer systems without a central server architecture). Thus, the above quoted portion of page 19 recites the entire discussion on page 19 of Jansen associated with a client-server system. The cited sentence does not disclose or suggest any operations performed by the central host. Furthermore the cited section does not disclose or suggest which security issues are addressed by the central host nor any processes by which those security issues are addressed. Page 19 of Jansen does not disclose or suggest a server that detects unwanted changes in the contents of a mobile application including comparing first and second instances of the mobile application.

Additionally, the Examiner makes the remarkable assertion that the Applicant's arguments are moot because the claims do not recite denial of service attacks. The Examiner is referring to the Applicant's arguments regarding section 2.1.2 of Jansen. However, the Applicant's arguments address the content of section 2.1.2 *as cited by the Examiner*, which describes denial of service attacks. However, the Applicant was describing the disclosure of Jansen, not the content of Applicant's claim. Applicant agrees that the claims do not describe denial of service attacks and therefore the Examiner's comment further supports Applicant's actual argument, namely that section 2.1.2 of Jansen does not disclose the limitations of claim 21. Applicant respectfully submits that claim 21, as well as claims 22-27, and 42-43, which depend from claim 21, are in condition for allowance.

Furthermore, Applicant notes that throughout the Examiner's response to Applicant's previous arguments, the Examiner recites limitations from cancelled claim 1, which are different from the limitations of pending claim 21.

Claim 28 stands rejected over Jansen. Claim 28 is directed to a method for verifying integrity of a jumping mobile application that includes storing, prior to a jump and at a server, a

first instance of a mobile application that jumps from a first host to a second host during execution, an instance of the mobile application including executable code for the mobile application. For at least the same reasons set forth above with respect to claim 21, claim 28 as well as claims 29-34, which depend from claim 28, are in condition for allowance.

Claim 35 stands rejected over Jansen. Claim 35 is directed to a computer program product that includes storing, prior to a jump and at a location other than a first host or a second host, a first instance of a mobile application that jumps from the first host to the second host during execution, an instance of the mobile application including executable code for the mobile application. For at least the same reasons as set forth above with respect to claim 21, claim 35 as well as claims 36-41, which depend from claim 35, are in condition for allowance.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 7 April 2006

Brian J. Gustafson
Reg. No. 52,978

Customer No. 26181
Fish & Richardson P.C.
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

50335601.doc